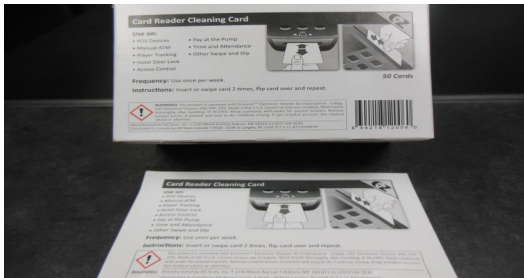


**GUIDE TO RECOGNIZING SKIMMING DEVICES ON YOUR ATMS**

Why is this guide Important? Informa is very aware of **many** skimming attacks on ATMs in Michigan and Ohio and with this rapid increase of skimming attacks your staff should inspect the machines daily for skimmers. Use this guide to help identify malicious hardware that may be installed on your institutions machines. Informa recommends that you also inspect your braille stickers and clean the dip card reader at the same time You can purchase cleaning cards from Informa ( pictured below) at (800)643-7489 for \$37.50 + taxes/shipping for a box of 50 cards.



**Create a process for weekly security inspections of your ATM/ITM.**

- Do inspections around card reader areas regularly.
- Check fascia of ATMs for unrecognizable devices.
- Check the keypad, dispenser, deposit area and ADA stickers for any irregularities and suspicious activity.





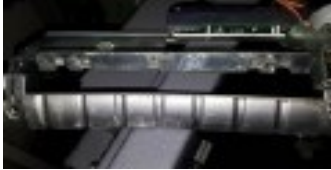

**Listed below are some of the different ways your machines can be manipulated with a skimming device.**

AREA TO CHECK	DEVICES TO LOOK FOR	EXAMPLES
Card Reader Bezel	Overlay skimmer (covers full exterior portion of card bezel)	
Card Reader Bezel	Partial overlay skimmer (covers part of the exterior portion of bezel)	
Card Reader Bezel	Partial overlay skimmer (covers part of exterior portion of bezel)	
Card Reader Bezel	Holes in bezel may be evidence of eavesdropping or tampering with anti-fraud solutions	
Card Reader	Deep insert skimmer (inside card reader)	
Card Reader	Shimming device (inside card reader)	
Card Reader	Unauthorized connections to card reader (eavesdropping)	

**Contact your Informa Sales Representative or call us @ 800-643-7489 for more information!**

AREA TO CHECK	DEVICES TO LOOK FOR	EXAMPLES	
Card Reader Bezel	Card Trapping Device		
Fascia	False Fascia, especially if fascia seems loose		
Fascia and side Panel	Holes in fascia and side panel could be a sign of: <ol style="list-style-type: none"> <li>1. Eavesdropping</li> <li>2. Deep insert removal attempt</li> <li>3. Black Box attack (if near EPP)</li> <li>4. Anti-skimming solution tampering</li> </ol> Hole may be covered in an attempt to conceal it	 	  
Dispenser and Depository Area	Various camera concealments, under molding or in the space between/beside the dispenser or depository slot		
Dispenser and Depository Area	Cash trapping devices		 
Above Monitor	Various camera concealments attached above the monitor		 
Under Monitor	Camera concealment attached to bottom of monitor		
Inset Area above Pin Pad	In curved/angled area of certain models (e.g. 6616 and 6622e)		
Pin Shield	Camera concealed under shield or shield modified to include a camera		

**Contact your Informa Sales Representative or call us @ 800-643-7489 for more information!**

AREA TO CHECK	DEVICES TO LOOK FOR	EXAMPLES
Fascia/Surround	Various camera concealments around fascia (could be anything unusual attached to the fascia or surround)	  
Pin Pad	Pin pad overlays	 
EPP	Tampering with or unauthorized removal of EPP	 
Communication/ Network Cabling	Unauthorized connections to network cables/router	  
USB hub/Dispense Cable	Peripheral device such as a laptop or handheld mobile device attached to USB hub or dispenser cable	 
Behind Dispenser Shutter	Unauthorized USB device, unauthorized CD ROM or hard drive compromise	
Envelope Depositories	Trapping Device	 
No-envelope Depositories	Trapping Device	
All area	Vandalism/visible damage such as chips, cracks, tool marks, glue/tape residue, shutter or belt damage may be evidence a fraud. Vandalism that takes an ATM out of service (e.g. Receipt paper jammed in card reader, glued card reader) should result in careful fraud inspection of sister ATMs.	    

Contact your Informa Sales Representative or call us @ 800-643-7489 for more information!